FYI.. As promised during the last HIPAA Security Subworkgroup meeting, I've extracted the following article concerning HIPAA Security and Privacy Rule relationships. The following article extract was copied from the attachment.

5 >> H I P A A / LAW: Special Legal Article

*** Final Security Regulations & How They Relate to the Privacy Rule ***

By Steve Fox & Rachel Wilson, Esqs.

The final security regulations promulgated under HIPAA (the "Security Rule") were published in the Federal Register on February 20, 2003 and will become effective for enforcement purposes on April 21, 2005. Recognizing the inextricable link between security and privacy, many covered entities are wondering how to integrate their security and privacy compliance initiatives, especially in light of the fact that the compliance date for the HIPAA Privacy Rule (the "Privacy Rule") is swiftly approaching (April 14, 2003).

In drafting the Privacy Rule, HHS was cognizant of the fact security measures are an integral part of insuring the privacy of information. The concept of security was incorporated into the Privacy Rule through the requirement that covered entities implement appropriate administrative, physical, and technical safeguards to insure the privacy of protected health information ("PHI"). While the Security Rule is only applicable to PHI in electronic form ("EPHI"), the scope of the Privacy Rule is much broader, mandating the use of security mechanisms to protect the privacy of PHI in both electronic and non-electronic form. Therefore, as it relates to integrating security and privacy compliance initiatives, many covered entities are (or should be) already half-way there - or at the very least, headed in the right direction, merely as a function of implementing HIPAA's privacy requirements.

Like the Privacy Rule, the Security Rule mandates the use of certain administrative, physical and technical and safeguards to protect confidentiality. However, in contrast to the Privacy Rule, which only requires the safeguards to be "adequate," the Security Rule actually sets forth specific standards that covered entities must implement in order to comply with the Security Rule. Essentially, the standards represent high-level security principles, which must be implemented by covered entities. How to implement the standards is left to each covered entity, although HHS offers "addressable" (optional) and "required" implementation specifications in most cases.

Covered entities do not have to change course with regard to the safeguards they plan to implement in order to comply with the Privacy Rule. But prudence would dictate that they begin to devise a plan for how to integrate the more comprehensive requirements set forth under the Security Rule into their current policies and procedures.

The first step in this process is to identify where EPHI is stored or maintained within the covered entity and how it is used and disclosed. The Security Rule is applicable to EPHI transmitted across the Internet as well as to information stored on computer hard drives and portable handheld devices. Next, covered entities should perform a gap analysis between current safeguards developed for HIPAA privacy compliance and any additional safeguards required to protect EPHI. Once the gaps are identified, covered entities can begin to develop a plan for gradually (sooner rather than later) filling in any gaps in security over the course of the next two years leading up to the compliance date for the Security Rule. However, as we have previously noted in past articles, since the so-called mini-security rule is already an integral part of the Privacy Rule, implementation of which is mandated now, covered entities must be in compliance by April 14, 2003. Therefore, under no circumstances should security concerns be delayed or postponed until the Security Rule compliance date.

Read past HIPAA Legal Q/A articles:
http://www.hipaadvisory.com/action/LegalQA/archives.htm

Steve Fox, Esq., is a partner at the Washington, DC office of Pepper Hamilton LLP. This article was co-authored by Rachel H. Wilson, Esq., of Pepper Hamilton. They may be reached at foxsj@pepperlaw.com. DISCLAIMER: This information is general in nature and should not be relied upon as legal advice.

Art Mark, CISA, CIA, CISSP, IT Security Branch
Planning & Consulting Division , Health & Human Services Data Center
State of California, (916) 454-7269, AMARK@HHSDC.CA.GOV

-----Original Message-----
From: HELEN NOVAK [mailto:HNOVAK@adp.state.ca.us]
Sent: Wednesday, April 09, 2003 8:46 AM
To: AMark@HHSDC.CA.GOV
Subject: Fwd: [hipaalert] HIPAAlert - Vol. 4, No. 2 - 3/12/03

Hi Art,

Attached is the HIPAAlert from Ken McInistry with the Risk Analysis for Security. It also has some other good articles about Security. Let me know what you think. Thanks again for picking up my stuff for me!

Helen